Performance Analysis of Physical Layer Security Attack on WiMAX System

[1]Rakesh Kumar Jha

[1,] SVNIT, Surat, Gujarat and SMVD University

Abstract— In this paper propose security issues and its solution for WiMAX network. Jamming and Scrambling is main security issues regarding Physical Layer. The lack of Physical infrastructure of wireless networks is inherently less secure. In this paper propose security issues and its solution for WiMAX network. Jamming and Scrambling is main security issues regarding Physical Layer. The lack of Physical infrastructure of wireless networks is inherently less secure. The performance analysis of the WiMAX system has been carried out for single and multicarrier jamming. It has been found that the performance of the system varies significantly with different jamming signals. The performance of the WiMAX system has been studied under the influence of the basis of Modulation schemes (QPSK, BPSK, 16 QAM and 64 QAM), Types of antennas (Sector antenna, Omni directional antenna and isotropic antenna) and Throughput on the basis of number of subcarriers destroyed. On the basis of simulation results and performance analysis found that the performance of BPSK and QPSK is better than other modulation scheme under single carrier jamming. WiMAX sector antenna gives better performance than isotropic and WiMAX Omni antennas. Throughput is reduced when data subcarriers are destroyed in uplink and downlink. Uplink is more sensitive to data subcarrier reduction compare to downlink. The performance of the downlink PUSC is better than uplink PUSC under the influence of the multicarrier jamming.

Keywords— WiMAX, Physical Layer, Network Layer, OPNET Modeler, QoS, Security

I. Introduction

Security has become a primary concern in order to provide protected communication in Wireless environment. It is know that the basic concept of communication is to send the information from source node to destination node.To successfully deploy multihop WiMAX networks, security is one of the major challenges that must be addressed. Another important issue is ways to support different services and applications in WiMAX networks. Nevertheless, observed that the security mechanism of IEEE 802.16 is mainly focused on security in the MAC layer, which may not be able to provide sufficient security in multihop scenarios and satisfy the requirements of emerging applications in WiMAX networks.

WiMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack including interception, fabrication, modification, and replay attacks [7]. Some vulnerabilities of WiMAX originate from flaws of IEEE 802.16 on which WiMAX is based. A lot of problems and flaws have been fixed in the enhanced version but WiMAX still has some exposes. In this section some possible threats or vulnerabilities will be reviewed.

Until the year 2000, users of the Internet accessed its contents primarily through wired, fixed infrastructure sites (e.g., universities, home dial-up connections, and corporate and government facilities). However, technology has evolved such that a significant number of users today access Internet services wirelessly. The cumulative result has created an information-centric society where users rely on network services in most aspects of their day-to-day life. The emerging wireless Internet architecture aims to continue the access revolution by supporting an increasing number of users at increased data rates, such that the user experience is similar to the experience from a wired, high-speed connection. A variety of wireless technologies have been proposed, both in standards organizations and by industry consortiums, to enable wireless network access.

II. Threats to The PHY layer

WiMAX security is implemented in the security sub-layer which is above the PHY layer. Therefore the PHY is unsecured [6] and it is not protected from attacks targeting at the inherent vulnerability of wireless links such as jamming, scrambling or water torture attack. WiMAX supports mobility, thus it is more vulnerable to these attacks because the attackers do not need to reside in a fixed place and the monitoring solutions presented below will be more difficult.h

1) Jamming attack: Jamming is described by M.Barbeau as an attack "achieved by introducing a source of noise strong enough to s significantly reduce the capacity of the channel" [6]. Jamming can be either intentional or unintentional. It is not difficult to perform a jamming attack because necessary information and equipment's are easy to acquire and there is even a book by Poisel [10] which teaches jamming techniques.

2) Scrambling attack: Also described in [5], scrambling is a kind of jamming but only provoked for short intervals of time and targeted to specific WiMAX frames or parts of frames at the PHY layer. Attackers can selectively scramble control or management information in order to affect the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more difficult to perform a scrambling attack than to perform a jamming attack due to "the need, by the attacker, to interpret control information and to send noise during specific intervals" [5].

3) Water torture attack: According to D. Johnson and J. Walker [3], this is also a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources.

4) Other threats: In addition to threats from jamming, scrambling and water torture attacks, 802.16 is also vulnerable to other attacks such as forgery attacks in which an attacker with an adequate radio transmitter can write to a wireless channel [3]. In mesh mode, 802.16 is also vulnerable to replay attacks in which an attacker resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process.

A Goal/Objective

The main Aim or goal of this thesis is to introduce the WiMAX network, discuss its Architecture along with the brief explanation of its Physical Layer and MAC (Media Access Control) Layer. Also the WiMAX network is implemented with the help of OPNET Modeler Networking tool, the performance analysis of the network model is to be done along with resource allocation. Optimization of the network model is also done on the basis of mutual collaboration between Subscriber Stations (SSs) and Base Stations (BSs). The WiMAX network Security is done on intrusion of Misbehaving Node attack. The Simulation parameters and Result analysis is finally done for the above described network models.

B The IEEE 802 Standard Families

Fig 1 shows the structure of the IEEE 802 standards family of ratified technologies. IEEE 802 primarily focuses on the Physical (PHY) and Media Access Control (MAC) layer specifications of the 7-layer Open Systems Interconnection (OSI) model context. Such standards in the IEEE 802 family include the IEEE 802.3 (wired Ethernet) standard, IEEE 802.1 (management) standard, IEEE 802.5 (token ring) standard, and the widely deployed IEEE 802.11 (wireless local area networks or WLAN) standard. WiMAX technology is primarily based on the IEEE 802.16 (Wireless Metropolitan Area Networks or WMAN) standard, while Bluetooth and ZigBee share similarities to some elements within the IEEE 802.15 standard.

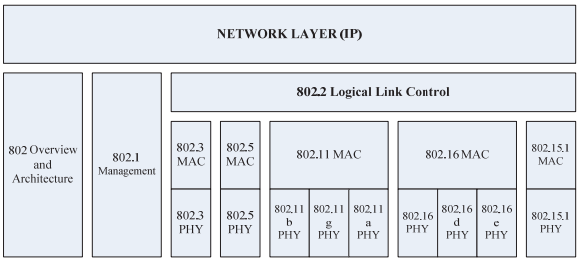

Fig 1 IEEE 802 Standards Family [8].

C Motivation

With the recent success and wide adoption of IEEE 802.11 WLAN technology, IEEE 802 has developed other standards that aim to take the emerging wireless Internet architecture even further. IEEE 802.16 technology is aimed at providing high-speed metropolitan area level access (similar to cellular infrastructure but advertised as a fraction of the cost). The IEEE 802.16e standard aims to provide WMAN access to mobile users moving at vehicular speeds.

D Coverage Area of WiMAX Network

A notional view of an IEEE 802 wireless Internet architecture is presented in Fig 2. Here, an IEEE 802.16 network is deployed to enable connectivity across a large area (on the order of a city, say around 100 km²).

Fig 2 Notional IEEE 802 wireless internet architecture [1].

Within the IEEE 802.16 network, users (known as Subscriber Stations or SS) may access Base Stations (BS) directly or gateways that bridge connections to other technologies (e.g., cellular, and wired infrastructure) may be employed.

In the figure, three locations are shown where connections are bridged between the IEEE 802.16 network and IEEE 802.11 access point networks. Here, the IEEE 802.16 network acts as a backhaul network while the IEEE 802.11 networks provide localized coverage to individual users or other gateway nodes (on the order of a city block, perhaps 10km²). The gateway nodes shown in the IEEE 802.11 network connects via bridges to IEEE 802.15 wireless personal area networks (WPANs). These IEEE 802.15 networks may provide micro-local coverage (on the order of 10 ft²) to devices such as cellular telephones, computer mice, or household appliances.

III.Parameter for Single Carrier Jamming

This section provides the implementation of radio network with a mobile jamming node. Interference (radio noise) can decrease the Signal-to-Noise Ratio (SNR) in a radio-based network. Different types of antennas, such as directional antennas, can improve the SNR in a network by increasing the effective signal strength at the receiver.

This model describes the effect of mobile jammer on receiver node with isotropic radiation pattern and direction antenna radiation pattern, the mobile jammer have straight trajectory.

A Network Model Components

This network model topology consists of three nodes:

- The Transmitter Node,
- The Receiver Node and
- The Mobile Jammer Node.

The Transmitter Node:

The Transmitter Node transmits at uniform strength in all directions. The transmitter node model consists of a packet generator module, a radio transmitter module, and an antenna module. The packet generator generates 1024-bit packets that arrive at the mean rate of 1.0 packets/second with a constant interarrival time. After they are generated, packets move through a packet stream to the radio transmitter module, which transmits the packets on a channel at 1024 bits/second using 100 percent of the channel bandwidth. The packets then pass from the transmitter through another packet stream to the antenna module. The node model for this Transmitter Node is shown in Fig 3.

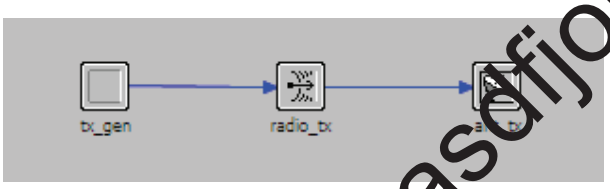

Fig 3 Radio Transmitter Node Model

The parameters set on the radio_tx node are shown in Fig 4; here the data rate is set to 1024 bps (i.e. 1 Kbps), also the bandwidth and minimum frequency is set to 10 KHz and 30 MHz respectively. The minimum frequency specifies the base frequency of the channel. The modulation on this transmitter node is set to BPSK (Binary Phase Shift Keying).

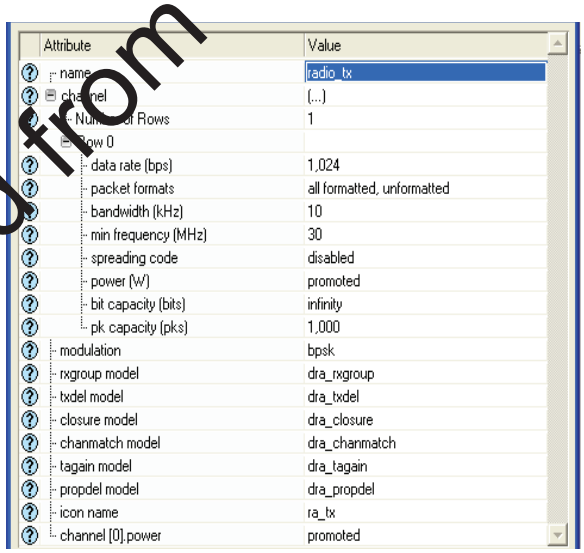

Fig 4 Simulation parameters on transmitter node

The Receiver Node:

The Receiver Node measures the quality of the signal emitted by the stationary transmitter node. It consists of an antenna module, a radio receiver module, a sink processor module, and an additional

processor module that works with the directional antenna. The node model for this Receiver Node is shown in Fig 5.

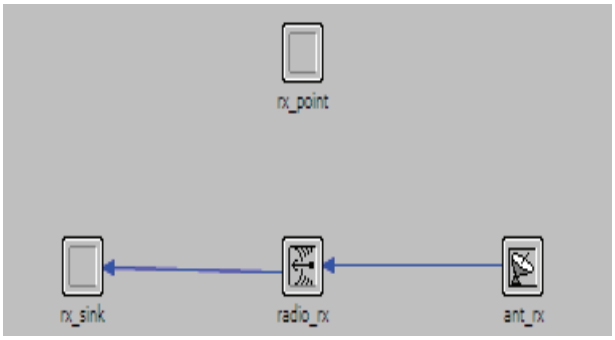

Fig 5 Radio Receiver Node Model

The Mobile Jammer Node:

The Mobile Jammer Node creates radio noise. The jammer's trajectory takes it in and out of the radio range of the receiver node, increasing and decreasing interference at the receiver. Like the stationary transmitter node, it consists of a packet generator module, a radio transmitter module, and an antenna module. Its behavior is similar to that of the stationary transmitter node, but channel power and signal modulation is different. These differences will make packets transmitted by the jammer node sound like noise to the receiver. The jammer node model is created from a copy of the transmitter node model.

Radio Network Model

Performance of model with Isotropic and Directional Antenna Radiation Pattern The model with mobile jammer having straight trajectory is shown in Fig 6; this model consists of radio transmitter node denoted by (tx), radio receiver node denoted by (rx) and mobile jammer node denoted by (jam) with straight trajectory shown.

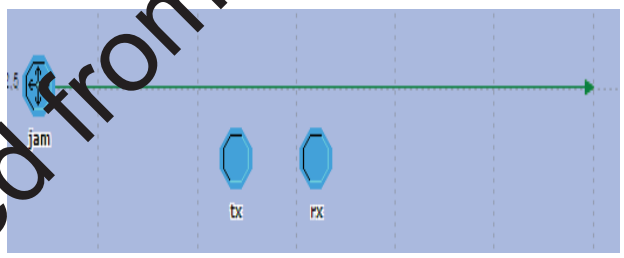

Fig 6 Network model with mobile jammer having straight trajectory

IV. Result Analysis (Single Carrier Jamming)

The simulation is done for 7 minutes, the graph of Bit Error Rate (BER) and Throughput (packets/sec) of the radio receiver node is shown in Fig 7 and Fig 8 respectively. There are two graphs in one figure, the upper graph in each figure indicates the results when isotropic radiation pattern is present at the radio receiver and the lower graph in both the figure indicates the results when directional antenna pattern is used.

From the graph of Bit Error Rate (BER) and Throughput (packets/sec), we can see that, when isotropic radiation pattern is used the average Bit Error Rate (BER) at the radio receiver increases and Throughput reduces due to large number of packet drops, which degrade the performance of the entire network.

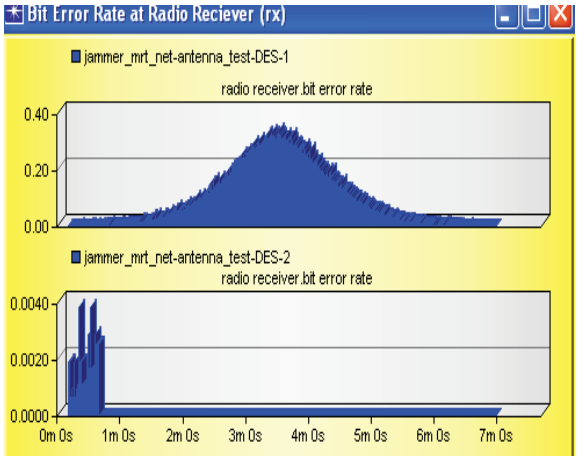

Fig 7 Bit Error Rate (BER) Performance at Radio Receiver

When the jammer node reaches nearer to receiver node the BER increases and when it passes away from the receiver the BER decreases.

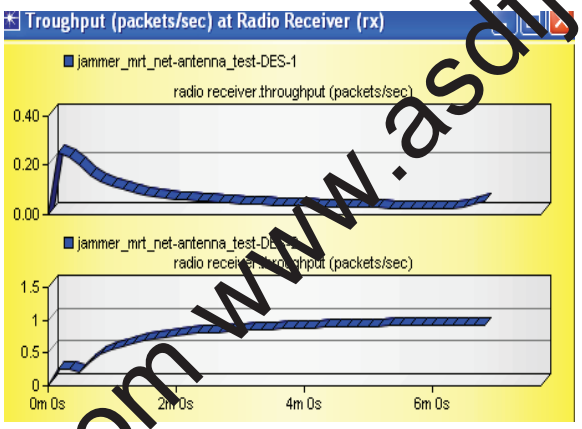

Fig 8: Throughput (packets/sec) at Radio Receiver

The maximum BER is shown as 0.35 which is high when jammer is very close to receiver node, and the Throughput is near about zero. When directional antenna pattern is used, the effect of jammer node does not affect the model, in this case the Bit Error Rate (BER) is very less which is near about zero and the Throughput (packets/sec) is maximum. Figure shows that the BER is 0.004 (~ 0.0) and Throughput is near about 1 packet/sec.

V. Simulation Parameters for Multi Carrier Jamming

Multi carrier jamming is difficult to simulate. In this thesis multi carrier jamming effect is modeled. Symbol duration is calculated by the following equation. In scalable OFDMA the symbol duration and sub carrier spacing is fixed. Number of sub carriers and bandwidth is changed to keep symbol duration and sub carrier spacing fixed.

$$T_s = T_b + T_g \quad \text{---------- (i)}$$

$$T_b = \frac{1}{\text{delta\_f}} \quad \text{---------- (ii)}$$

$$delta\_f = \frac{bandwidth}{subcarriers} \times n \quad \text{-------- (iii)}$$

$$T_g = \frac{T_b}{8} \quad \text{---------- (iv)}$$

Where, n= sampling factor
delta_f=tone spacing

T_s = symbol duration

T_g = guard time

T_b = useful symbol duration

Equation (IV) shows number of sub carriers is proportional to bandwidth of channel for scalable OFDMA. It is multi carrier scheme. Multi carrier jamming scenario is shown in Fig.9.

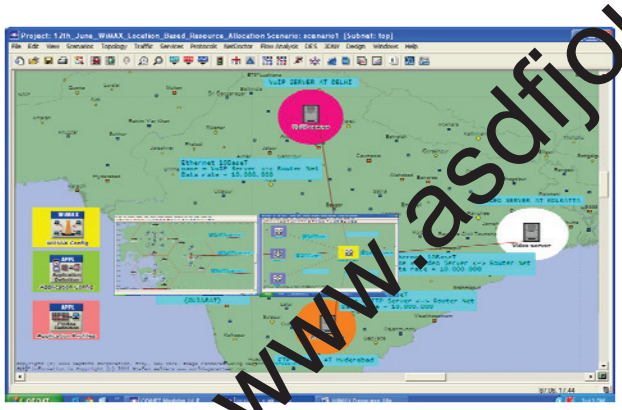

Fig. 9 Scenario used to simulate multi carrier jamming.

In this scenario fixed NLOS is considered. There are two subscriber stations. Application and profile node is used to create an application. Parameters associated with PUSC are shown in Table 1.

Table 1 PUSC Permutation Scheme for Uplink

	512	1024
Number of sub channels	17	35
Data sub carriers used	272	560
Pilot sub carrier	136	280
Left-guard sub carriers	52	92
Right-guard sub carriers	51	91

Downlink PUSC permutation scheme is also used in simulation. Numbers of data, pilot and guard sub carriers required for scalable OFDMA are shown in the Table 2.

Table 2 PUSC Permutation Scheme for Downlink

	128	512	1024	2048
Number of sub channels	3	15	30	60
Data sub carriers used	72	360	720	1440
Pilot sub carrier	12	60	120	240
Left-guard sub carriers	22	46	92	184
Right-guard sub carriers	21	45	91	183

Steps involved in multi carrier jamming simulation are described below.

1. Take the scenario as shown in Fig 9 Set the application which is to be examined under jamming effect. Select parameters for the same.

2. Now choose number of subscribers and base stations. Set their attributes according to application.

3. Set WiMAX attributes of all subscribers and base stations. Set the symbol duration according to standards.

4. Set permutation mode as per the simulation criteria.

5. Now simulate the scenario and see the throughput and delay.

6. Take new scenario as shown in Fig 9 and repeat step number 1 to 4. Reduce number of data or pilot or guard sub carriers in uplink or downlink as per simulation criteria but keep symbol duration, sub carrier spacing and bandwidth same as the first scenario.

7. Now simulate this scenario and compare the throughput and delay result with previous result.

By following above steps multi carrier jamming effect can be simulated and results can be noted down. The simulation parameters are given in Table 3

Table 3 Simulation parameters and their values

	Parameter	Value
1	Bandwidth	5 MHz for 512 sub carriers 10 MHz for 1024 sub carriers
2	Symbol duration	102.86 μseconds
3	Sub carrier spacing	10.94 KHz
4	Frame duration	0.005 seconds
5	Duplexing technique	TDD
6	Frame preamble (symbols)	1
7	Transmit transition gap	106 micro seconds
8	Receive transition gap	60 micro seconds
9	Base frequency	5 GHz
10	Sampling factor	28/25
11	Efficiency mode	Physical layer enabled

In Mobile WiMAX, the FFT size is scalable from 128 to 2,048. Here, when the available bandwidth increases, the FFT size is also increased such that the sub carrier spacing is always 10.94 kHz. This keeps the OFDM symbol duration, which is the basic resource unit, fixed and therefore makes scaling have minimal impact on higher layers. A scalable design also keeps the costs low. The sub carrier spacing of 10.94 kHz was chosen as a good balance between satisfying the delay spread and Doppler spread requirements for operating in fixed and mobile environments. This sub carrier spacing can support delay-spread values up to 20 micro seconds and vehicular mobility up to 125 km per hour when operating in 3.5GHz. A sub carrier spacing of 10.94 kHz implies that 128, 512, 1,024, and 2,048 FFT are used when the channel bandwidth is 1.25MHz, 5MHz, 10MHz, and 20MHz, respectively. 2-11 GHz is used for Fixed NLOS and 2-6 GHz is used for mobile NLOS. It should, however, be noted that mobile WiMAX may also include additional bandwidth profiles. For example, a profile compatible with WiBro will use an 8.75MHz channel bandwidth and 1,024 FFT. This obviously will require different sub carrier spacing and hence will not have the same scalability properties. The number of sub carriers may be 512, 1024 and 2048. Data sub carriers, Null sub carriers and Pilot sub carriers are also given for 512, 1024 and 2048 sub carriers. The WiMAX configuration node is used to configure WiMAX properties. IEEE 802.16e uses fixed and mobile NLOS. There are two sub carrier permutation modes FUSC (full usage sub carrier) and PUSC (partial usage sub carrier).

Uplink and downlink both can use different permutation modes in single application. In uplink PUSC sub carrier permutation is given in Table 1 [16]. Same way in Downlink PUSC sub carrier permutation is given in Table 2 [1]. In Simulation depending on number of sub carriers and permutation scheme used parameters are chosen from the given tables.

VI. Result and Analysis (Multiparae Carrier Jamming)

In this scenario two subscriber stations and one base station are there. Any application can be used to simulate multi carrier jamming. In this scenario Video conferencing application is chosen. Number of sub carriers chosen for this application is 512 and bandwidth is 5 MHz for this application. The symbol duration is 102.86 micro seconds and sub carrier spacing is 10.94 KHz. Uplink and downlink both use PUSC. Take new scenario as shown in Fig. 9 and keep all the parameters same except number of sub carriers and bandwidth. Now choose 1024 sub carriers and 10 MHz the results for scalability property are shown in Fig. 10 and Fig. 11. Simulation time is set to 300 seconds. Throughput and delay of whole system is considered in the results. The system throughput is the sum of all data rates that are delivered to all terminals in a network. Delay is time taken by a packet to reach its destination starting from the time it leaves the source.

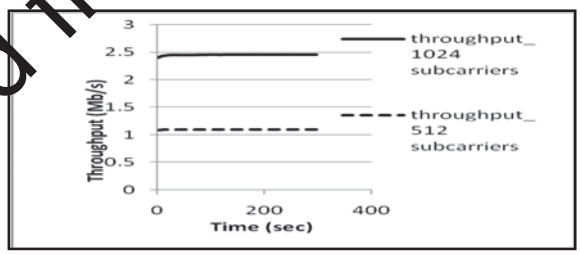

Fig. 10 Throughput vs. simulation time

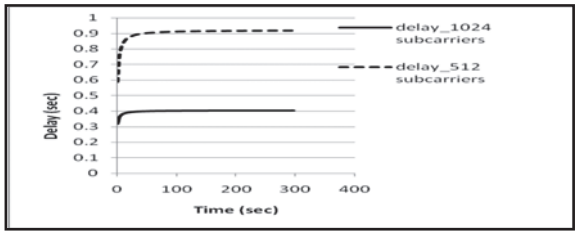

Fig 11 Delay vs. simulation time

New scenario is taken as shown in Fig. 9 to simulate multi carrier jamming effect. Sampling factor n is 28/25 and number of sub carriers are 1024. This scenario is run for 300 seconds. Bandwidth is 10 MHz, sub carrier spacing is 10.94 KHz same as second scenario. Data sub carriers in uplink PUSC and downlink PUSC are 560 and 720 respectively. Number of sub channels in uplink PUSC and downlink PUSC are 35 and 30 respectively. Now follow the steps that are already mentioned in simulation section to simulate multi carrier jamming. Procedure to simulate multi carrier jamming is already mentioned. In uplink the effect of data sub carrier reduction is more compare to that in downlink. Results for uplink multi carrier jamming are shown in Fig. 12 and Fig 13. Here Fig. 10 and Fig 11 show the effect of scalability property of OFDMA on throughput and delay. Fig 10 shows the throughput for 512 and 1024 sub carriers. Bandwidth is different for both the case. 1024 sub carriers produce more throughput than 512 sub carriers. Fig 11 shows delay. The symbol duration and sub carrier spacing keep same for both 512 and 1024 sub carriers but the number of sub carriers and bandwidth is changed. Fig. 12 and fig. 13 show the effect of number of data sub carrier reduction on throughput and delay in uplink. Throughput is decreased as numbers of data sub carriers are destroyed.

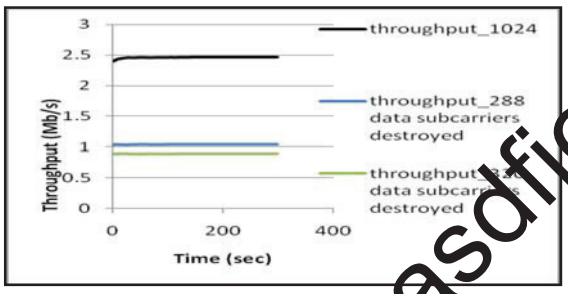

Fig 12 throughput vs. simulation time for uplink

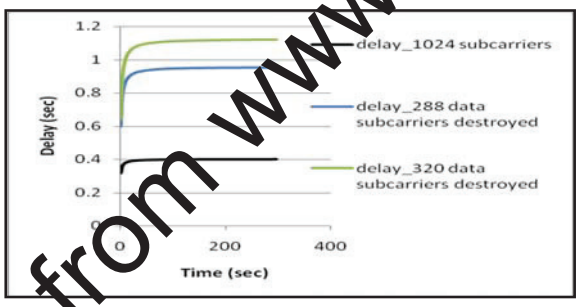

Fig 13 Delay vs. simulation time for uplink

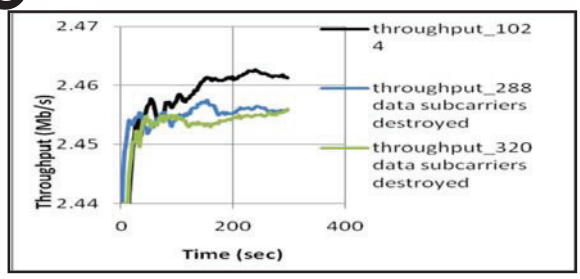

Fig. 14 Throughput vs. simulation time for downlink

In this thesis only data sub carriers are destroyed and effect is noted down. If pilot sub carriers are destroyed then channel estimation becomes very difficult. Multi carrier jamming effect on throughput and delay in downlink is shown below. Fig. 12 shows throughput with all data sub carriers, with 288 destroyed data sub carriers, with 320 destroyed data sub carriers. Throughput vs. simulation time in downlink is shown in Fig 14. Delay vs. simulation time in downlink is shown in Fig 15. The performance of downlink PUSC is better than uplink PUSC. More number of data sub carriers present in downlink

PUSC than uplink PUSC is first reason. The second reason is downlink PUSC scheme itself which is described in detail in theory part.

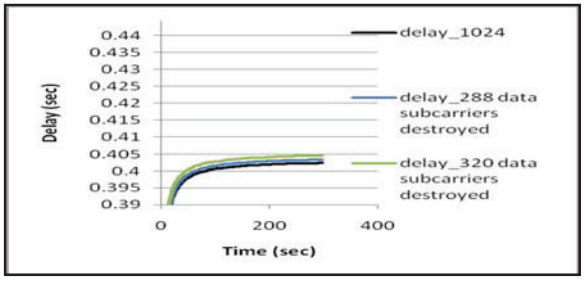

Fig. 15 Delay vs. simulation time for downlink

VII. CONCLUSIONS

The performance of BPSK and QPSK is better than other modulation scheme under single carrier jamming. WiMAX sector antenna gives better performance than isotropic and WiMAX Omni antennas. Throughput is decreased when data sub carriers are destroyed in uplink and downlink. Throughput is reduced means BER is increased. Delay is increased when data sub carriers are destroyed in uplink and downlink. Uplink is more sensitive to data sub carrier reduction compare to downlink. Both single carrier jamming and multicarrier jamming are destructive in nature. Single carrier jamming can be detected easily compared to multi carrier jamming. The performance of the downlink PUSC is better than uplink PUSC under the influence of the multi carrier jamming. Multi carrier jamming effects are modeled in this thesis using particular algorithm which is already mentioned earlier.

References

[1] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, Fundamentals of WiMAX Understanding Broadband Wireless Networking, 1-63, 27 Sep, 2007.

[2] Rakesh Kumar Jha,Upena D Dala, "A Journey on WiMAX and its Security Issues", International Journal of Computer Science and Information Technologies, Vol. 1(4) , 2010, 256-263

[3] Syed Ahson, Mohmmad Ilyas, Syed Ahson, Mohammad Ilyas, WiMAX Standards and Security. Boca Raton: CRC Press, 2008.

[4] S. A. Vakin, L. N. Shustov, R. H. Dunwell, Fundamentals of Electronic Warfare, Artech House, 384 pp., 2001.

[5] Simon Haykin, Michael Moher, Modern Wireless Communications, Prentice-Hall, U.S.A, 560 pp., 2005.

[6] Rakesh Kumar Jha, Hardik Patel, Upena D Dalal, Wankhede A Vishal, "WiMAX System Simulation and Performance Analysis under the Influence of Jamming",WET Vol 1,Issue , pp 20-26,2010

[7] ILYAS, S. A. (2008). WiMAX Standards and Security. London: CRC Press.

[8] Gilberto Flores Lucio, Marcos Paredes-Farrera, Emmanuel Jammeh, Martin Fleury, Martin J. Reed, Electronic Systems Engineering Department, University of Essex, "OPNET Modeler and Ns-2: Comparing the Accuracy Of Network Simulators for Packet- Level Analysis using a Network Test bed", 2005.

[9] White paper by Motorola, "WiMAX Security for Real-World Network Service Provider deployments", 2007.

[10] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El-Hennawy, "WiMAX Security", 22nd International Conference on Advanced Information Networking and Applications, 2008.

[11] Boris Makarevitch, "Jamming Resistant Architecture for WiMAX Mesh Network", communications Laboratory Helsinki University of Technology, 2007.

[12] LUO Cuilan, "A Simple Encryption Scheme Based on WiMAX", Department of Electronics Jiangxi University of Finance and Economics Nanchang, China, 2009.

[13] Frank Hsieh, Fan Wang, Amitava Ghosh, "Link Performance of WiMAX PUSC", Networks Advanced Technologies, Home & Networks Mobility, Motorola Inc., WCNC 2008.

[14] Mika Husso, "Performance Analysis of a WiMAX System under Jamming", Thesis Helsinki University of Technology, 2006.

[15] Jesús Manuel González de Jesús, "Exploring Jamming Attacks using OPNET® 12.0", 2007.

[16] IEEE 802.16 Working Group. IEEE 802.16-2004 Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems IEEE Standard for Local and Metropolitan Area Networks[S]: IEEE Computer Society Press.

[17] IEEE 802.16 Working Group. IEEE 802.16e-2005 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for combined Fixed and Mobile Operation in Licensed Bands[S]: IEEE Computer Society Press.

[18] Rakesh Kumar Jha, Upena D Dalal and Suresh V Sankar, "A Performance of Security Aspect in WiMAX Physical Layer with Different Modulation Schemes" Advances in Computing, Communication and Control, International Conference, ICAC3 2011, Mumbai, India, January 28-29, 2011. Proceedings, Vol 125,PP 433-440.